UW Whitewater Police

	Information Security Incident Response	Number: 93.2	No. Pages: 2
	Author: SueAnn Farnsworth		
	Approved By: Chief Kiederlen	Effective Date: 7/1/2022	Revised Date: New	Revision number: New

I.   Purpose

The purpose of this policy is to establish the minimum requirements to report an Information Security (IS) incident in the UW- Whitewater Police Department (UWWPD) or on one of its assets, and the subsequent required actions when an incident occurs.

II.   Definitions

Data: Information collected, stored, transferred or reported for any purpose, whether electronic or hard copy.

Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples include denial of service attack, threat from a widespread malware attack in which systems are vulnerable, etc.

IT Asset: Equipment or software used to manage, process, or store police data and is used in the course of accomplishing the UWWPD mission. This includes but is not limited to all university or department owned or leased:

- Desktop, laptop and server computers and associated IT infrastructure;
- Mobile devices and portable computing equipment;
- Network devices such as firewalls, routers, switches, and wireless access points;
- Software; and
- Multi-function devices, printers and scanners.

LASO: Local Agency Security Officer

Threat: Any circumstance or event with the potential to adversely impact the organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

III. Policy

It is the policy of the UW-Whitewater Police Department (UWWPD) that any Information Security Incidents must be reported. Incidents must be reported to ICIT, the on-call supervisor, and the LASO.

It is the policy of UWWPD that they will follow UW System Administrative Policy 1033: Information Security- Incident Response.

IV. Procedure

A. Employees should contact the UW- Whitewater IT Help Desk (X 4357), the on-call supervisor, and the LASO (SueAnn Farnsworth- X 3180) as soon as they become aware of, or suspect, a potential or actual information security incident. This includes, but is not limited to:

1. Reporting all lost or stolen IT assets, including personally owned devices which contain UWWPD data or information
2. Reporting physical intrusion into secure areas
3. Discovery of malware or unauthorized access to IT/UWWPD assets

B. If the help desk is closed due to a holiday, weekend or overnight hours, the employee will contact the on-call supervisor who will report it to IT. The on-call supervisor will also report the incident to the LASO.

C. The LASO will report the incident to WI DOJ, CIB TSCC, or DCI WSIC; depending on which department they can reach first.